Not for publication until released by the Subcommittee

Prepared Statement of
Robert J. Brandewie
Director, Defense Manpower Data Center

Before the House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations

Oversight Hearing on "The Status of the Department of Veterans' Affairs Smart Card Initiative(s)"

October 6, 2004

ROBERT J. BRANDEWIE
Director
Defense Manpower Data Center (DMDC)
Monterey, California

Mr. Brandewie currently serves as the Director, Defense Manpower Data Center, a field activity reporting to the Office of the Secretary of Defense (Personnel and Readiness). He is responsible for oversight of the largest and most comprehensive automated personnel data base in DoD, management of a dozen major operational DoD programs, supervision of a multi-disciplinary staff of approximately 750, and administration of the Monterey office. Recently, Mr. Brandewie has led DMDC efforts: to redesign the Department's benefits and entitlements database for the new TRICARE system; to design and field a comprehensive web authentication capability for DoD; to develop and field an identification card and biometric based force protection system; and to design and develop the Common Access Smartcard as the new DoD identification card.

Mr. Brandewie received an M.A. in Administrative Sciences from Yale University in 1972 and a B.A. in Psychology from the University of Connecticut in 1970. Mr. Brandewie was twice awarded the Presidential Rank Award of Meritorious Executive (in 1997 and in 2002); has twice been the recipient of the Secretary of Defense Medal for Meritorious Civilian Service, and was awarded the Secretary of Defense Exceptional Civilian Service Award. He was selected as one of the FED100 for 2003, an award based on influencing the course of Federal information technology. Mr. Brandewie was selected as a career member of the Senior Executive Service in May of 1993.

Robert J. Brandewie
Defense Manpower Data Center
400 Gigling Rd.
Seaside, CA 93955

Work: 831 583-2400
Cell: 831 320-6551
robert.brandewie@osd.pentagon.mil

Good morning ladies and gentleman. As the Director of the Defense Manpower Data Center (DMDC), I am responsible for the development, fielding, and maintenance of a number of Department of Defense (DoD)-wide systems. Today, I will discuss the DoD smart card initiative known as the Common Access Card, commonly referred to as the CAC. In addition, I will address DoD's efforts with the National Institute of Standards and Technology (NIST) to facilitate the fulfillment of the requirements directed in the Homeland Security Presidential Directive 12 (HPSD-12).

DoD recognized the importance of strengthening the identification and authentication process in the mid 1990's, given the increasing ease with which credentials could be counterfeited or fraudulently obtained. Also, the Department recognized the increasing importance of network based communication, and the rise in the attractiveness of e-business and e-government transactions for efficiency and cost effectiveness. The response in both cases was to strengthen the business process for the identification and credentialing of our military members, civilian employees, and family members. The Department began work in November of 1999 to modify the DoD Identification Card from a relatively low technology card to a smart card with an integrated circuit chip (ICC). The new smart card would be an authentication token for the military member or employee, and also, contain Public Key Infrastructure (PKI) cryptographic keys and certificates. The Department made a conscious decision to use the smart card as an authentication device instead of a data storage device for three reasons: (1) minimize the problem of synchronizing the card and the database, (2) minimize the concern of always chasing a larger capacity card, and (3) most importantly, mitigate any risk for our military members were they to be captured in time of hostilities.

Such a card was critical to the secure use of the network capabilities, and therefore, would increase security while at the same time enabling more efficient and effective web-based transactions for a variety of DoD business processes. The initial test cards were produced in December of 2000 and full production of this new card, called the CAC, began in September of 2001. By July of 2003, the full infrastructure was rolled out to 945 sites in 27 countries and the program was fully implemented. Today, more than 5.5 million CACs have been issued at the rate of more than 10,000 per day. Currently, about 3.2 million DoD active and reserve military members, civilian employees and DoD contractors carry a valid CAC. This includes the 1.75 million Army, Navy, Air Force, and Marine Corps active duty and Selected Reserve members in the DoD; the 49,500 Coast Guard members in the Department of Homeland Security (DHS); the 6,000 Public Health Service (PHS) members in the Department of Health and Human Services (HHS); and the 250 National Oceanographic and Atmospheric Administration (NOAA) members in the Department of Commerce (DOC).

At the same time, and just as importantly, DoD has focused its Personnel Identity Protection program on the business process; securely identity proofing and vetting individuals and binding their identity to a credential, the CAC, at issuance. The process of performing secure, upfront identity proofing and vetting is the foundation upon which a sound credentialing infrastructure is built. To do less weakens the resulting credential, as well as the trust that can be placed in the credential.

The first step in the Personnel Identity Protection process is strong authentication of the individual. This requires a business process that provides sufficient evidence of identity and a face-to-face interaction between the individual and a trusted agent.

Providing sufficient evidence of identity should include, at a minimum, checks of public records, background investigations, and examination of primary documents to name a few. The second step in the process is to bind that confirmed identity to a management system. A credential is the best linkage to a Personnel Identity Protection system. Binding the credential to the individual is the third step in the process. The use of biometrics and Personal Identification Numbers (PINs) are good mechanisms to bind the credential to the person, and both are used in the DoD program. This step fixes the individual's identity to the credential from that point forward. The credential then becomes an identity proxy and a token for providing logical and/or physical access. Step four is the authentication of the credential at all physical and logical access points. Step five is revoking the credential, as close to real-time as possible, when the individual's affiliation is terminated or when the credential is lost, stolen, or compromised (similar to what happens in the credit card industry). The last step in the Personnel Identity Protection system is to safeguard personal identity information from unwarranted disclosure. In an age where identity theft is the fastest growing white collar crime, this last step is critically important.

There are characteristics of the Department's issuance process that contribute to its strength and mitigate the vulnerabilities of any credentialing system. First, the credentialing system is linked to a central repository of affiliated people entitled to the Department's credential. This repository is fed by approximately 75 authoritative sources of military member and civilian personnel information in the DoD. This authoritative source of identity and affiliation information is the Defense Eligibility Enrollment Reporting System (DEERS). Second, the issuers of credentials are vetted before they are

given access to the system by the Defense Security Service (DSS). Third, the issuers of credentials are authenticated using their CACs (requiring a PIN), their biometric (a fingerprint), and the workstation being used. Likewise, the cards that they are issuing are authenticated against a card management system and a logistics portal. All of these factors must pass security scrutiny and be authenticated and approved before a card is issued. Fourth, the issuers of credentials are not able to add new people to the repository because their eligibility for a DoD credential must be independently verified by an authoritative data source. Finally, the issuers of credentials do not grant privileges.

The CAC is used for authentication of identity, logical access to DoD networks and systems, and for physical access to DoD buildings and facilities, the latter being the application that is the slower of the three to be implemented. Reforms in electronic business (to include paperless contracting, wide-area workflow, and other procurement and finance applications), travel re-engineering, and expanded use of the government-wide commercial purchase card program coupled with information assurance for data and identity authentication have presented new opportunities to use smart card technology as an enabling tool for enhancing business processes. The CAC is used for various business applications such as a replacement for passwords, food service, deployment/warrior readiness, and manifesting. DMDC continues to work with the Components and other Defense Agencies to develop specific applications to enhance military readiness and improve the quality of life.

As the use of the CAC for applications expands and the technology becomes more advanced, additional space on the card is required. In March of 2005, DoD will move to a 64K contact card to meet emerging requirements and to be compliant with the

Government Smart Card Interoperability Specification (GSC-IS) v2.1. In response to requests from the physical access community, DoD anticipates piloting contactless smart card technology by end of Summer/Fall 2005. DoD is also working towards an enterprise biometrics solution for an additional layer of security on the card. The Department has been capturing digital fingerprints on military personnel for approximately four years and has prints on almost all uniformed members in its central repository. As part of CAC issuance, DoD captures two fingerprints on military, civilian and contractor personnel, if we do not already have them. At re-issuance, the system performs a fingerprint check between the live person and the database to ensure it is the same person. In the event of a non-match, which can occur for a number of reasons, the operator is required to take additional steps to verify identity before issuing a card. DoD is changing its business processes to have digital fingerprints captured at enlistment processing stations for the purpose of background checks by the Federal Bureau of Investigation (FBI). The fingerprints would also be sent to the central repository used in the credential issuance process. This permits the Department to ensure that the person processed for enlistment is the same individual showing up at basic training, further strengthening the Personnel Identity Protection process. While considerable investigation of the utility of other biometric measures is ongoing in the DoD, under the auspices of the DoD Biometrics Management Office (BMO), current plans for the CAC are limited to fingerprints. To introduce a new card (64K) or other technology change (contactless) into the system, a little over three years is required to implement and replace all active cards. To change data or applets (e.g., biometrics) stored on the card, much less time is required since it is possible to securely change certain software on the card using post

issuance capabilities.

DMDC maintains the identification information known as the Defense Enrollment Eligibility Reporting System (DEERS), for generating Uniformed Service sponsor and family member benefits, entitlements, and identification credentials. The Real-time Automated Personnel Identification System (RAPIDS) is used to issue the credential of affiliation with DoD, and it relies on the information stored in DEERS. The CAC serves as the assertion of identity and is authenticated against the DEERS database, global directory services, or DoD PKI services in real-time whenever possible. The granting of logical and physical access privileges remains a local policy and a business operation function of the local facility, but must function in concert with Personnel Identity Protection policies and procedures.

There is not an easy solution to the worldwide problem of knowing, with absolute certainty, exactly who each person is. Many organizations tend to focus on the latest technology such as smart card technology, PKIs, biometrics, and sophisticated physical and logical access control systems. The technology is important; however, the risks are large, and it is not enough when protecting the identity and privacy of individuals. Through the use of a strong and rigorous issuance process, followed by strong electronic authentication of the credential whenever it is used, it is far more difficult for someone to steal another individual's identity. The Defense Biometrics Identification System (DBIDS), Defense Cross-Credentialing Identification System (DCCIS), and Defense National Visitors System (DNVS) meet the objective of the Personnel Identity Protection program.

DBIDS is a theater, or regional based force protection system developed initially

by DMDC at the request of United States (US) Forces Korea. In brief, it uses cards, photographs, and fingerprints to control access to all gates to US facilities on the Korean peninsula. All personnel having access are required to go through a registration process where biometrics are captured and cards are issued to those who do not already have either a CAC or some other DoD issued credential. A "one-to-many" fingerprint check is made to identify anyone already in the database. A server based database, downloaded to the gates, is available throughout Korea, and is designed to operate in the absence of communications, if necessary. Gate guards have wireless handheld devices capable of scanning a card and determining whether it is genuine and valid. The devices bring up a photograph of the person from the database, and perform a fingerprint check in a matter of seconds. Any or all of these checks can be done depending on the threat conditions. The system also notifies guards if someone should be barred or even arrested. Subsequently, this system was fielded in Europe and Kuwait. Plans are underway for fielding this system in Japan, Qatar, and Forts Hood and Polk.

The Defense Cross-Credentialing Identification System (DCCIS) is an initial proof-of-concept for testing a standards-based (X.509) implementation of existing PKIs, and potentially, other commercial identity schemas. This proof-of-concept proposes to resolve the interoperability difficulties between DoD and its commercial partners. DCCIS would be used in instances where there is a reciprocal requirement for enrolling and identifying personnel and granting them various access privileges to both physical sites and logical networks, but where there is also a requirement to maintain control and access of an organization's own data. DCCIS enables participating DoD facilities to achieve strong and interoperable identity verification and authentication of participating

contractor/private sector personnel who present a company-issued trusted credential. This system provides a means to share identity authentication information across organizational network infrastructure boundaries. The ultimate goal is to create a "federated" system between the DoD and its industry partners that reflects the interests of each party in retaining control of its own policies; including the access control policies at the local level.

The Defense National Visitors System (DNVS) enables participating DoD facilities to perform physical authentication procedures on DoD personnel presenting CACs for entrance into DoD facilities. It is a web-based system that verifies physical access credentials with a sub-second response time. In addition, DNVS can be DCCIS enabled. In this case, a participating DNVS facility would connect with DCCIS member organization databases in order to authenticate visiting personnel from those organizations.

I would like to conclude my statement with a few remarks about the importance of using standards-based commercial products whenever possible. The ability to write specifications in terms of well-defined and accepted national and international standards, and to have laboratories that can test products and certify that these standards have been met, ultimately reduces the cost to the users and promotes interoperability between and among Federal agencies, industry, business partners, and other countries. There has been a concerted effort to use such standards in the development and implementation of the CAC. The General Services Administration (GSA) and the National Institute of Standards and Technologies (NIST) have been critical partners in this process. As a result, it is very easy for other organizations to adopt all or part of what DoD has done

with the CAC. DoD has worked and will continue to work with other Federal agencies wanting assistance with similar programs, or to provide information on valuable lessons learned. For example, DoD and the Department of Veterans' Affairs (VA) have been in contact to share technical approaches to credentialing over the past two years. There have been discussions of DoD hosting VA infrastructure as well as the transfer of VA expertise in using credentials in the medical business space to DoD. Additional conceptual discussions of the DoD issuing a VA credential to departing DoD members promises cost savings, in addition to strengthening the transfer of a member's identity from organization to organization. These concepts can reduce costs as well as provide better service to our common beneficiaries.

Thank you for the opportunity to address the Subcommittee.